IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Cr. No. 06-20033-STA**
	)	
DANIEL SCOTT OGDEN,	)	
	)	
Defendant.	)	

ORDER ADOPTING THE MAGISTRATE JUDGE'S REPORT AND RECOMMENDATION DENYING DEFENDANT'S THIRD MOTION TO SUPPRESS AND OVERRULING DEFENDANT'S OBJECTIONS

Before the Court is Defendant Daniel Scott Ogden's Objections to the Report and Recommendation of the Magistrate Judge Denying Defendant's Third Motion to Suppress Evidence (D.E. # 170) filed on September 29, 2008. The Government responded to Defendant's objections (D.E. # 191) on October 14, 2008. For the reasons set forth below, the Report and Recommendation is **ADOPTED** and Defendant's objections are **OVERRULED**.

BACKGROUND

According to the affidavit of Special Agent Stephen Lies, which was attached to the search warrant at issue in this case, Defendant, a thirty-four year old resident of Memphis, Tennessee, began an internet relationship with a minor female ("SS") from California on March

17, 2005.[1] SS was 15 when she initially engaged in email exchanges with Defendant.[2] During the course of their relationship, she allegedly emailed him pictures of herself "standing fully nude, smiling, or lying on her bed."[3] According to SS, the Defendant told her he saved those pictures to an external drive.[4] After SS turned sixteen, she and Defendant began discussing the possibility of having sexual intercourse.[5] Agent Lies asserted in his affidavit that those conversations included graphic and specific descriptions of sex acts that the Defendant wished to perform.[6]

On September 16, 2005, Defendant flew to California to meet SS.[7] After picking him up from the airport, SS drove the Defendant to a hotel in San Francisco, where they allegedly repeatedly engaged in sexual intercourse.[8] At some point while Defendant and SS were in each other's company, her parents discovered their relationship and called her on her cell phone.[9] Subsequently, SS decided to return home.[10] Later that day, Defendant appeared at SS's home

---

[1] D.E. # 63 Ex. A at 7-8.

[2] *Id*. at 7.

[3] *Id*.

[4] *Id*.

[5] *Id*.

[6] *Id*.

[7] *Id*. at 8.

[8] *Id*.

[9] *Id*.

[10] *Id*.

and was arrested.[11]

Approximately a week later, Special Agent Lies visited Defendant's residence in Memphis and spoke with his grandmother, the owner of the house.[12] She invited investigators into her home and discussed her broken water heater with them.[13] According to Lies, Defendant's

grandmother wanted to show them the damage done by the water heater and took them to a back bedroom where the Defendant stayed.[14] There, Lies observed an external hard drive on the night stand, as well as other external media on the bed and in an open bag on the floor.[15] The Defendant's grandmother told the investigators that there was also a computer stored in the attic.[16] The investigators collected the Gateway desktop computer from the attic ("the desktop"), the external hard drive, and the diskettes found on the bed and in the bag on the floor, and transported them back to their office.[17]

On October 13, 2005, Magistrate Judge Diane Vescovo signed a search warrant permitting the search of the desktop, the external hard drive, and the diskettes.[18] The warrant

---

[11] *Id*.

[12] *Id*.

[13] *Id*.

[14] *Id*.; D.E. # 70 at 76.

[15] D.E. # 63 Ex. A at 8.

[16] *Id*.

[17] *Id*. at 9.

[18] *Id*. at 10-11.

was executed on October 21, 2005.[19] Defendant was eventually charged with various counts of production, possession, and receipt of child pornography and using the telephone/internet system to persuade a minor female to engage in sexual acts which were illegal under California law.

Defendant filed his Third Motion to Suppress (D.E. # 97) on July 13, 2008. The Government responded in opposition (D.E. # 110) on July 25, 2008. The Court referred the Motion to the United States Magistrate Judge for report and recommendation on July 31, 2008. Magistrate Judge Vescovo conducted a hearing on the Motion on September 19, 2008. Both Defendant and the Government had the opportunity at that hearing to question Special Agent Lies about the search and seizure of Defendant's computer equipment and storage media. At the conclusion of the hearing, Judge Vescovo ruled from the bench and found that there was no flagrant disregard for the search warrant and denied the Motion to Suppress. Judge Vescovo did not issue a written order. Under the Federal Rules, Defendant had ten (10) days in which to file objections to Judge Vescovo's ruling, that is, until October 3, 2008.

Defendant filed his Objections to the Magistrate Judge's Report and Recommendation (D.E. # 170) on September 29, 2008. At that time, the transcript of the September 19 hearing had yet to be completed. With trial set for the following day, Defendant moved to continue the trial (D.E. # 167) citing in part the lack of opportunity for review of the Magistrate Judge's ruling. The Court denied the motion to continue and commenced jury selection on September 30, 2008. Following a four-day trial, the jury returned a verdict of guilty as to all nine counts against Defendant.

[19] D.E. # 63 at 39.

STANDARD OF REVIEW

Where a Magistrate Judge considers dispositive motions including motions to suppress evidence in a criminal case, the Magistrate Judge may only issue recommendations for the disposition of the motion pursuant to subparagraph 28 U.S.C. § 636(b)(1)(B).[20] The Court must review *de novo* any portions of a Magistrate Judge's report to which objections are made.[21]

ANALYSIS

Having reviewed *de novo* Defendant's motions and objections, the Government's responses, and the entire record of the proceeding before Judge Vescovo, the Court adopts the Magistrate Judge's Report and overrules Defendant's objections. Defendant contends that the Magistrate Judge erred in finding that the Government did not exceed the scope of the search warrant in this case. As a result the Magistrate Judge also erred in not recommending that all evidence seized pursuant to the search warrant be suppressed. More specifically, Defendant argues that the Government seized several files stored on his computer equipment and storage media, which were not covered by the search warrant. These items included music, soft-core commercial adult pornography, and photographs of clothed minors, or of minors with breasts and buttocks visible, and family photographs. None of these computer files met the definition of child pornography covered by the statutes under which Defendant was indicted. Defendant concedes that the Government must first review items stored in computers and other media to determine whether the files contain evidence of illegal activity. However, according to

[20] 28 U.S.C. § 636(b)(1)(B).

[21] 28 U.S.C. § 636(b)(1)(C).

Defendant, the Government seizure of the individual files actually occurred after its initial review, not at the time of its seizure of the computer devices containing the files. Applying this reasoning to the facts in this case, Defendant contends that the Government "seized" every file from all of the computer equipment and storage media taken from Defendant's residence. Many of those files were not covered in the search warrant, and so the seizure improperly exceeded the scope of the search warrant. Therefore, all of the files must be suppressed as evidence.

The Government has responded that Defendant has failed to show that the examining agent acted with flagrant disregard for the terms of the search warrant. While the Government grants that search warrants involving child pornography stored as computer files present a complex question of law, the Government avers that there are no grounds to suppress the evidence in this case. Searching agents have the authority to look in any place where the evidence sought may be found. The methods employed in executing search warrants are left to the searching agent's discretion as long as the methods are reasonable. Contrary to Defendant's argument, Special Agent Lies seized all of the computer equipment, not each individual file. This was proper because all of the computer equipment and storage devices were within the scope of the search warrant. Special Agent Lies thus acted reasonably in executing the search warrant, and his examination of each file on Defendant's computers and storage media was reasonable and necessary. Therefore, the scope of the warrant was not exceeded and the evidence should not be suppressed.

The Court finds that Defendant's objection is without merit. As an initial matter, Defendant's brief contains no citation to any legal authority whatsoever. Accordingly, it is not clear what legal grounds Defendant has for his motion or his theory concerning the

Government's search and seizure of his computers and storage devices. At the hearing before Judge Vescovo, Defendant stated, "we are asking that because the government interpreted the warrant as allowing them to seize everything, they did seize everything, and that their interpretation was overbroad and that therefore everything should be suppressed."[22] The Court has rejected Defendant's argument that the search warrant itself was overbroad on separate occasions.[23] Here Defendant's primary argument appears to be that the Government's execution of the warrant was overbroad, that is, the Government engaged in a general search of the seized computer devices. Accordingly, the Government investigators flagrantly disregarded the parameters of the search warrant when it seized computer files, which contained no evidence of child pornography. Defendant bases this contention on his theory that the Government "seized" the files for purposes of the Fourth Amendment, not when the Government removed the computer devices from Defendant's residence but when it searched the files for contraband. Without further support, this theory is unavailing. The Government has responded that it did not seize individual computer files but the devices which stored the files. According to the Government, the fact that the seized devices contained files which were not contraband did not invalidate the search.

In the search and seizure of computers containing files with no relationship to illegal activities, "[a] search does not become invalid merely because some items not covered by a

---

[22] Mot. Hr'g Tr. 7:11-16, Sept. 19, 2008.

[23] Order Granting in Part and Den. in Part Def.'s Mot. to Suppress (D.E. # 79), May 28, 2008; Order Den. Def.'s Mot. for *Franks* H'rg and for Suppression of Evidence (D.E. # 125), August 2, 2008.

warrant are seized."[24] In fact, investigators armed with a valid search warrant may seize entire computers, computer systems, or storage media where there is probable cause to believe that the computer devices contain evidence of child pornography.[25] This practice is reasonable for investigators because of "the technical difficulties of conducting a computer search in a suspect's home."[26] For a variety of reasons, the Government must sometimes search many files, or as the First Circuit has expressed it, uncover "some needles in the computer haystack," in order to locate child pornography stored on a computer.[27] Indeed the practice of requiring narrowly-defined searches of computer files for child pornography poses the risk to investigators of failing "to cast a sufficiently wide net to capture the evidence sought."[28]

For example, someone who possesses child pornography can easily save an image as a computer file with an innocuous name in order to hide its true contents. The Ninth Circuit has recognized this very real obstacle to investigators conducting searches of computers for

---

[24] *Guest v. Leis*, 255 F.3d 325, 334 (6th Cir. 2001) (quoting *U.S. v. Henson*, 848 F.2d 1374, 1383 (6th Cir.1988)). Another district court in the Sixth Circuit has ably discussed the problems associated with the search and seizure of computers in child pornography cases but in the slightly different context of the overbreadth of a search warrant. *See U.S. v. Kaechele*, 466 F. Supp. 2d 868, 885-89 (E.D. Mich. 2006). Defendant argues here that the Government in its execution of the warrant conducted an overbroad search and seizure of the files contained in Defendant's computer devices, not that the warrant itself was overbroad.

[25] *E.g., U.S. v. Adjani*, 452 F.3d 1140, 1149-50 (9th Cir. 2006); *U.S. v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006) ("a computer search may be as extensive as reasonably required to locate the items described in the warrant"); *U.S. v. Upham*, 168 F.3d 532, 535 (1st Cir.1999) ("[T]he seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images"); *U.S. v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997).

[26] *Guest*, 255 F.3d at 335.

[27] *Upham*, 168 F.3d at 535.

[28] *Adjani*, 452 F.3d at 1149-50 (9th Cir. 2006).

contraband files:

> Computer files are easy to disguise or rename, and were we to limit the warrant to such a specific search protocol, much evidence could escape discovery simply because of [a defendant's] labeling of the files documenting [his or her] criminal activity. The government should not be required to trust the suspect's self-labeling when executing a warrant.[29]

In the case at bar, the Government alleges that some of the illegal images found on Defendant's computer devices were given names such as "finger," "peekaboo," "766," and "100_1685," to name a few. None of these file names on their face, however, would openly and obviously denote child pornography. Therefore, a searching agent must reasonably access these and other files for the purpose of determining whether they contain the child pornography described in the warrant affidavit.

To hold otherwise would require courts to suppress the fruits of nearly every investigative search of computers in child pornography cases. Common sense dictates that even computers containing illegal files will also contain legal computer files. Under Defendant's theory, the Government would impermissibly seize legal computer files nearly every time it seized a computer where there was probable cause to believe that the computer contained evidence of child pornography. This is clearly not the applicable standard. Having already found that the search warrant was proper and not overbroad at an earlier phase in the case, the Court finds that Defendant has failed to show that the Government investigative agents acted improperly in the execution of the search warrant.

In light of the foregoing, the Court has found no authority for the proposition that a

---

[29] *Id.*

search and seizure procedure like the one used in the case at bar was improper or represents a blatant disregard for the terms of the search warrant. Therefore, the Magistrate Judge's report is **ADOPTED**, and Defendant's Objections are **OVERRULED**.

IT IS SO ORDERED.

s/ S. Thomas Anderson
S. THOMAS ANDERSON
UNITED STATES DISTRICT JUDGE

Date: November 18th, 2008.